

WHAT IS CLAIMED IS:

1 A method of encrypting a shared document, comprising:
2 under control of an encryption server system,
3 generating a ECC public/private key pair for the encryption server
4 system;
5 under control of a client system,
6 requesting a Java® encryption applet from the encryption server
7 system;
8 requesting an encryption server system EEC public key from the
9 encryption server system;
10 under the control of the encryption server system,
11 transmitting the Java® encryption applet to the client system over a
12 secure channel;
13 transmitting the encryption server system EEC public key to the client
14 system over a secure channel;
15 under control of a client system,
16 receiving the Java® encryption applet from the encryption server
17 system over a secure channel;
18 receiving the encryption server system EEC public key from the
19 encryption server system over a secure channel;
20 installing the Java® encryption applet on the client system;
21 running the Java® encryption applet on the client system to generate a
22 Triple DES symmetric key;
23 encrypting a clear text document with the Triple DES symmetric key,
24 thereby creating a cipher text document;
25 creating a relationship between the cipher text document and the Triple
26 -DES symmetric key;
27 encrypting Triple DES symmetric key with the encryption server EEC
28 public key, thereby creating an encrypted Triple DES symmetric
29 key;
30 creating a relationship between the cipher text document and the
31 encrypted Triple DES symmetric key;
32 transmitting the cipher text document to the encryption server system;

33 transmitting the encrypted Triple DES symmetric key to the encryption
34 server system;
35 transmitting the relationship between the cipher text document and the
36 encrypted Triple DES symmetric key to the encryption server
37 system;
38 under the control of the encryption server system,
39 storing the cipher text document in a storage medium;
40 storing the encrypted Triple DES symmetric key in a storage medium;
41 and
42 storing the relationship between the cipher text document and the
43 encrypted Triple DES symmetric key in a storage medium.

1 2. The method of claim 1, wherein the secure channel is an SSL channel.

1 3. The method of claim 1, wherein the Java® encryption applet is
2 installed on a browser.

1 4. The method of claim 3, wherein the browser is the Internet Explorer®
2 or the Netscape Navigator®.

1 5. The method of claim 1, wherein the cipher text document is
2 transmitted from the client system to the encryption server system using FTP, and the
3 encrypted Triple DES symmetric key is transmitted to the encryption server system via
4 HTTP.

1 6. The method of claim 1, wherein the cipher text document is
2 transmitted from the client system to the encryption server system using FTP, and the
3 document is decrypted upon arrival at the server.

1 7. The method of claim 1, further comprising the steps of:
2 under the control of the encryption server system,
3 storing the relationship between the cipher text document and the
4 encrypted Triple DES symmetric key by making a first and a
5 second entry in a correlation table, the first entry representing the

encrypted Triple DES symmetric key, and the second entry representing the cipher text document.

1 10. The method of claim 1, further comprising the steps of:
2 under the control of the encryption server system,
3 decrypting the encrypted Triple DES symmetric key with the
4 encryption server system EEC private key, thereby creating a
5 decrypted Triple DES symmetric key;
6 decrypting the cipher text document with the decrypted Triple DES
7 symmetric key, thereby creating a clear text document; and,
8 storing the clear text document on the encryption server system.

11. The method of claim 7, further comprising the steps of:
under the control of the encryption server system,
using the first entry in the correlation table to retrieve the encrypted
Triple DES symmetric key;
decrypting the encrypted Triple DES symmetric key using the
encryption server system EEC private key, thereby creating a
decrypted Triple DES symmetric key;
decrypting the cipher text document with the decrypted Triple DES
symmetric key, thereby creating a clear text document;
storing the clear text document on a storage medium; and
making a third entry in the correlation table, thereby creating a
relationship between the cipher text document, the clear text
document and the encrypted Triple DES symmetric key.

1 12. The method of claim 11, wherein the third entry is the clear text
2 document.

1 13. The method of claim 11, wherein the third entry is a pointer to the
2 clear text document.

1 14. The method of claim 7, further comprising the steps of:
2 under control of the client system,
3 requesting the cipher text document from the server;
4 under control of the encryption server system,
5 using the first entry in the correlation table to retrieve the encrypted
6 Triple DES symmetric key;
7 decrypting the Triple DES symmetric key using the encryption server
8 system EEC private key, thereby creating a decrypted Triple DES
9 symmetric key;
10 inserting the Triple DES symmetric key into a Java® decryption
11 applet;
12 sending the Java® decryption applet to the client system over a secure
13 channel;
14 sending the cipher text document to the client system;
15 under control of the client system,
16 installing the Java® decryption applet on the client system; and,
17 decrypting the cipher text document using the Java® decryption applet,
18 thereby creating a clear text document.

1 15. The method of claim 14, wherein the Java® decryption applet is
2 installed on a browser.

1 16. The method of claim 15, wherein the browser is the Internet Explorer®
2 or the Netscape Navigator®.

1 17. The method of claim 10, further comprising the steps of:
2 under control of the client system,
3 requesting the clear text document from the server;
4 under control of the encryption server system,
5 generating a Triple DES symmetric key;
6 encrypting the clear text document with the Triple DES symmetric
7 key, thereby creating a cipher text document;

inserting the Triple DES symmetric key into a Java® decryption applet;
sending the Java® decryption applet to the client system over a secure channel;
sending the cipher text document to the client system;
under control of the client system,
installing the Java® decryption applet on the client system; and,
decrypting the cipher text document using the Java® decryption applet,
thereby creating a clear text document.

18. The method of claim 17, wherein the Java® decryption applet is browser.

19. The method of claim 18, wherein the browser is the Internet Explorer® or the Netscape Navigator®.

20. The method of claim 11, further comprising the steps of:

under control of the client system,

requesting the clear text document from the server;

under control of the encryption server system,

generating a Triple DES symmetric key;

encrypting the clear text document with the Triple DES symmetric key, thereby creating a cipher text document;

inserting the Triple DES symmetric key into a Java® decryption applet;

sending the Java® decryption applet to the client system over a secure channel;

sending the cipher text document to the client system;

under control of the client system,

installing the Java® decryption applet on the client system; and,

decrypting the cipher text document using the Java® decryption applet,

thereby creating a clear text document.

21. The method of claim 20, wherein the Java® decryption applet is browser.

24 encrypting Triple DES symmetric key with the encryption server EEC
25 public key, thereby creating an encrypted Triple DES symmetric
26 key;
27 creating a relationship between the cipher text document and the
28 encrypted Triple DES symmetric key;
29 transmitting the cipher text document to the encryption server system;
30 transmitting the encrypted Triple DES symmetric key to the encryption
31 server system;
32 transmitting the relationship between the cipher text document and the
33 encrypted Triple DES symmetric key to the encryption server
34 system;
35 under the control of the encryption server system,
36 storing the cipher text document in a storage medium;
37 storing the encrypted Triple DES symmetric key in a storage medium;
38 and
39 storing the relationship between the document and the Triple DES
40 symmetric key in a storage medium.

25. An encryption system for shared documents, comprising:
1 an encryption server system and a client system;
2 the encryption server system,
3 generating a ECC public/private key pair for the encryption server system;
4 transmitting the Java® encryption applet to the client system over a secure
5 channel;
6 transmitting the encryption server system EEC public key to the client
7 system over a secure channel;
8 storing the encrypted document in a storage medium;
9 storing the encrypted Triple DES symmetric key in a storage medium;
10 storing the relationship created between the document and the Triple DES
11 symmetric key in a storage medium;
12 a client system,
13 requesting a Java® encryption applet from the encryption server
14 system;

1 22. The method of claim 21, wherein the browser is the Internet Explorer®
2 or the Netscape Navigator®.

1 23. The method of claim 1, further comprising the steps of:
2 under the control of the encryption server system,
3 decrypting the encrypted Triple DES symmetric key with the
4 encryption server system EEC private key, thereby creating a
5 decrypted Triple DES symmetric key; and,
6 decrypting the cipher text document with the decrypted Triple DES
7 symmetric key, thereby creating a clear text document.

1 24. A method of encrypting a shared document, comprising:
2 under control of a client system,
3 requesting a Java® encryption applet from the encryption server
4 system;
5 requesting an encryption server system EEC public key from the
6 encryption server system;
7 under the control of the encryption server system,
8 transmitting the Java® encryption applet to the client system over a
9 secure channel;
10 transmitting the encryption server system EEC public key to the client
11 system over a secure channel;
12 under control of a client system,
13 receiving the Java® encryption applet from the encryption server
14 system over a secure channel;
15 receiving the encryption server system EEC public key from the
16 encryption server system over a secure channel;
17 installing the Java® encryption applet on the client system;
18 running the Java® encryption applet on the client system to generate a
19 Triple DES symmetric key;
20 encrypting a clear text document with the Triple DES symmetric key,
21 thereby creating a cipher text document;
22 creating a relationship between the cipher text document and the Triple
23 DES symmetric key;

16 requesting an encryption server system EEC public key from the
17 encryption server system;
18 receiving the Java® encryption applet from encryption server system
19 over a secure channel;
20 receiving the encryption server system EEC public key from
21 encryption server system over a secure channel;
22 installing the Java® encryption applet on the client system;
23 running the Java® encryption applet on the client system to generate a
24 Triple DES symmetric key;
25 encrypting a clear text document with the Triple DES symmetric key,
26 thereby creating a cipher text document;
27 creating a relationship between the cipher text document and the Triple
28 DES symmetric key;
29 encrypting Triple DES symmetric key with the encryption server EEC
30 public key, thereby creating an encrypted Triple DES symmetric
31 key;
32 creating a relationship between the cipher text document and the
33 encrypted Triple DES symmetric key;
34 transmitting the cipher text document to the encryption server system;
35 transmitting the encrypted Triple DES symmetric key to the encryption
36 server system;
37 transmitting the relationship between the cipher text document and the
38 encrypted Triple DES symmetric key to the encryption server
39 system.

1 26. The encryption system of claim 25, wherein the encryption server
2 system is further comprised of:
3 storing the relationship between the cipher text document and the encrypted
4 Triple DES symmetric key by making a first and second entry in a correlation table, the first
5 entry represents the encrypted Triple DES symmetric key, and the second entry represents the
6 cipher text document.

1 27. The encryption system of claim 26, wherein the encryption server
2 system is further comprised of:

making a third entry in the correlation table, wherein the third entry represents the clear text document;

creating a relationship between the cipher text document, the encrypted Triple DES symmetric key, and the clear text document; and,

storing the relationship between the cipher text document, the encrypted Triple DES symmetric key, and the cipher text document.

28. An encryption system for shared documents, comprising:
an encryption server system and a client system;
the encryption server system,

using the first entry in the correlation table to retrieve the encrypted Triple DES symmetric key;

decrypting the Triple DES symmetric key using the encryption server system EEC private key, thereby creating a decrypted Triple DES symmetric key;

inserting the Triple DES symmetric key into a Java® decryption applet;

sending the Java® decryption applet to the client system over a secure channel;

sending the cipher text document to the client system;

under control of the client system,

requesting the cipher text document from the server;

under control of the encryption server system,

installing the Java® decryption applet on the client system; and,

decrypting the cipher text document using the Java® decryption applet, thereby creating a clear text document.

29. An encryption system for shared documents, comprising:

an encryption server system and a client system;

under control of the encryption server system,

generating a Triple DES symmetric key;

encrypting the clear text document with the Triple DES symmetric key, thereby creating a cipher text document;

inserting the Triple DES symmetric key into a Java® decryption applet;
sending the Java® decryption applet to the client system over a secure channel;
sending the cipher text document to the client system;
under control of the client system,
requesting the clear text document from the server;
installing the Java® decryption applet on the client system; and,
decrypting the cipher text document using the Java® decryption applet,
thereby creating a clear text document.

30. An encryption system for shared documents, comprising:
an encryption server system and a client system;
the encryption server system,
generating a ECC public/private key pair for the encryption server system;
transmitting the Java® encryption applet to the client system over a secure channel;
transmitting the encryption server system EEC public key to the client system over a secure channel;
storing the cipher text document in a storage medium;
storing the encrypted Triple DES symmetric key in a storage medium;
storing the relationship created between the cipher text document and the encrypted Triple DES symmetric key in a storage medium;
using the first entry in the correlation table to retrieve the encrypted Triple DES symmetric key;
decrypting the Triple DES symmetric key using the encryption server system EEC private key, thereby creating a decrypted Triple DES symmetric key;
inserting the encrypted Triple DES symmetric key into a Java® decryption applet;
sending the Java® decryption applet to the client system over a secure channel;
sending the cipher text document to the client system;

24 decrypting the encrypted Triple DES symmetric key using the
25 encryption server system EEC private key, thereby creating a
26 decrypted Triple DES symmetric key;
27 sending the cipher text document to the client system;
28 generating a Triple DES symmetric key;
29 encrypting the clear text document with the Triple DES symmetric
30 key, thereby creating a cipher text document;
31 a client system,
32 requesting a Java® encryption applet from the encryption server
33 system;
34 requesting an encryption server system EEC public key from the
35 encryption server system;
36 receiving the Java® encryption applet from encryption server system
37 over a secure connection;
38 receiving an encryption server system EEC public key from the
39 encryption server system over a secure channel;
40 installing the Java® encryption applet on the client system;
41 running the Java® encryption applet on the client system to generate a
42 Triple DES symmetric key;
43 encrypting a clear text document with the Triple DES symmetric key,
44 thereby creating a cipher text document;
45 creating a relationship between the cipher text document and the Triple
46 DES symmetric key;
47 encrypting Triple DES symmetric key with the encryption server EEC
48 public key, thereby creating an encrypted Triple DES symmetric
49 key;
50 creating a relationship between the cipher text document and the
51 encrypted Triple DES symmetric key;
52 transmitting the document encrypted with the Triple DES symmetric
53 key from the client system to the encryption server system;
54 transmitting the Triple DES symmetric key encrypted with the
55 encryption server system EEC public key from the client system to
56 the encryption server system;

57 transmitting the relationship between the cipher text document and the
58 encrypted Triple DES symmetric key to the encryption server
59 system;
60 requesting the cipher text document from the server;
61 installing the Java® decryption applet on the client system; and,
62 decrypting the cipher text document using the Java® decryption applet,
63 thereby creating a clear text document; and,
64 requesting the clear text document from the server.

PA 3116007 v1